



UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
-----------------	-------------	----------------------	---------------------	------------------

10/807,180

03/24/2004

Katsuhiko Hashimoto

108391-00038

4177

4372 7590 04/26/2007
ARENT FOX PLLC
1050 CONNECTICUT AVENUE, N.W.
SUITE 400
WASHINGTON, DC 20036

EXAMINER

TRAORE, FATOUMATA

ART UNIT

PAPER NUMBER

2109

SHORTENED STATUTORY PERIOD OF RESPONSE	MAIL DATE	DELIVERY MODE
--	-----------	---------------

3 MONTHS

04/26/2007

PAPER

Please find below and/or attached an Office communication concerning this application or proceeding.

If NO period for reply is specified above, the maximum statutory period will apply and will expire 6 MONTHS from the mailing date of this communication.

Office Action Summary	Application No. 10/807,180	Applicant(s) HASHIMOTO ET AL.	
	Examiner Fatoumata Traore	Art Unit 2109	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- .. Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- .. If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- .. Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

- 1) ☒ Responsive to communication(s) filed on 24 March 2004.
- 2a) ☐ This action is **FINAL**. 2b) ☒ This action is non-final.
- 3) ☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

- 4) ☒ Claim(s) 1-30 is/are pending in the application.
- 4a) Of the above claim(s) _____ is/are withdrawn from consideration.
- 5) ☐ Claim(s) _____ is/are allowed.
- 6) ☒ Claim(s) 1-30 is/are rejected.
- 7) ☐ Claim(s) _____ is/are objected to.
- 8) ☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

- 9) ☐ The specification is objected to by the Examiner.
- 10) ☒ The drawing(s) filed on 24 March 2004 is/are: a) ☒ accepted or b) ☐ objected to by the Examiner.
Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).
Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).
- 11) ☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

- 12) ☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).
- a) ☐ All b) ☐ Some * c) ☐ None of:
1. ☐ Certified copies of the priority documents have been received.
 2. ☐ Certified copies of the priority documents have been received in Application No. _____.
 3. ☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).
- * See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

- | | |
|---|---|
| 1) <input checked="" type="checkbox"/> Notice of References Cited (PTO-892) | 4) <input type="checkbox"/> Interview Summary (PTO-413)
Paper No(s)/Mail Date. _____ |
| 2) <input type="checkbox"/> Notice of Draftsperson's Patent Drawing Review (PTO-948) | 5) <input type="checkbox"/> Notice of Informal Patent Application |
| 3) <input checked="" type="checkbox"/> Information Disclosure Statement(s) (PTO/SB/08)
Paper No(s)/Mail Date <u>03/24/2004</u> . | 6) <input type="checkbox"/> Other: _____ |

DETAILED ACTION

1. This is in response of the original fling of March 24, 2004. Claims 1-30 are pending and have been considered bellow.

Information Disclosure Statement

2. The information disclosure statement filed March 24, 2004 fails to comply with 37 CFR 1.98(a)(3) because it does not include a concise explanation of the relevance, as it is presently understood by the individual designated in 37 CFR 1.56(c) most knowledgeable about the content of the information, of each patent listed that is not in the English language. It has been placed in the application file, but the information referred to therein (specifically document JP 9-204361) has not been considered.

Claim Rejections - 35 USC § 102

The following is a quotation of the appropriate paragraphs of 35 U.S.C. 102 that form the basis for the rejections under this section made in this Office action:

A person shall be entitled to a patent unless –

(b) the invention was patented or described in a printed publication in this or a foreign country or in public use or on sale in this country, more than one year prior to the date of application for patent in the United States.

3. Claim 29 is rejected under 35 U.S.C. 102(b) as being anticipated by Imamura et al (US 2002/0116551).

Claim 29: Imamura et al discloses a data storage device that ensures the secrecy and the security of data recorded on a memory medium comprising:

- i. A first writing that includes writing a predetermined unencrypted data into a nonvolatile first data area from which data can be read and written after resetting the first data area (at step 105, a check is performed to determine whether the security are is in the initial state. When the security is in the initial state, when no device identifier has been recorded in the security area, the process then advances to step 108, whereat the reading of data from the medium and the writing of data to it are permitted. It is assumed that the security level has not been set) (page 4, paragraph 74), and writing key data into a nonvolatile second data area into which data can be written but can not be read (when the two device identifiers match, the process advances to step 308, whereat a check is performed to determine whether writing in accordance with the write address information is permitted. When the write address information has been set, the process advances to step 309 whereat the writing of data is permitted but the reading of data is inhibited) (page 5, paragraph 90);
- ii. Inhibiting the reading and the writing of the first data (when the two device identifiers do not match, the security is not released and reading/writing of data is inhibited) (page 4, paragraph 77);
- iii. A second writing that includes writing temporary key data into a nonvolatile key register, into which data can be written but can not be read

when the reading and the writing of the first data are inhibited (when the two device identifiers match, the process advances to step 308, whereat a check is performed to determine whether writing in accordance with the write address information is permitted. When the write address information has been set, the process advances to step 309 whereat the writing of data is permitted but the reading of data is inhibited) (page 5, paragraph 90);

iv. And authorizing the reading or writing of the first data when the temporary key data match the key data (when the two device identifiers match, the process then advances to step 108, whereat the security is released and the reading of data from the medium and the writing of data to it are permitted) (page 4, paragraph 76), whereas inhibiting the reading and the writing of the first data when the temporary key data do not match the key data (when the two device identifiers do not match, the security is not released and reading/writing of data is inhibited) (page 4, paragraph 77).

4. Claim 30 is rejected under 35 U.S.C. 102(b) as being anticipated by **Nakamura et al** (US 6457126).

Claim 30: **Nakamura et al** discloses a storage device an encrypting decrypting device and method of accessing a non-volatile memory comprising:

- i. Encrypting and writing the key data as encrypted data, into a nonvolatile second data area that stores second data that can be read and written (writing means for encrypting data using the first to third encrypting keys stored in said first to third encrypting keys storage means, and writing the encrypted data in a non-volatile memory) (column 5, lines 45-49);
- ii. And reading and decrypting the encrypted data so as to acquire the key data, wherein the key data acquired by decrypting the encrypted data are written as the temporary key data into the key register at the second writing (Reading means for reading data from the non-volatile memory, decrypting the read data using first to third encrypted keys and outputting data) (column 5, lines 45-49).

Claim Rejections - 35 USC § 103

5. The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negated by the manner in which the invention was made.

6. Claims 1-3, 8, 10 are rejected under 35 U.S.C. 103(a) as being unpatentable over anticipated by **Chiba et al** (US 4589064) in view of **Imamura et al** (US 2002/0116551).

Claim 1: **Chiba et al** discloses a system for controlling key storage unit with control access to main storage device comprising:

A nonvolatile first data area that stores first data that are not encrypted and that can be read and written (the data processing apparatus includes a main storage unit) (column 2, lines 6-7);

A nonvolatile first key data area that stores first key data that can be written but can not be read (the data processing apparatus includes a main storage unit and a key storage unit for storing a main storage protection key) (column 2, lines 6-8);

A nonvolatile second key data area that stores second key data that can be written but can not be read (the data processing apparatus includes a main storage unit and a key storage unit for storing a main storage protection key) (column 2, lines 6-8);

But does not explicitly disclose a controller that allows reading or writing of the first data when the first key data matches with the second key data. However, **Imamura et al** discloses a data storage device that ensures the secrecy and the security of data recorded on a memory medium, which further encloses a controller that allows reading or writing of the first data when the first key data matches with the second key data (a controller for comparing said first identifier with said second identifier, and controlling access to said memory medium for data reading and/or writing according to a relationship between said first identifier and said second identifier) (page 1, paragraph 12) (when first identifier and the

second identifier match, the controller permits access to the memory medium for the reading and writing of data) (page 1, paragraph 13). Therefore, it would have been obvious for one having ordinary skill in the art at the time the invention was made to add a controller to Chiba et al's disclosure. One would have been motivated to control the device in order to prevent an unauthorized person to access the content of the device.

Claim 2: Chiba et al and Imamura et al disclose a system for controlling key storage unit with control access to main storage as in claim 1 above, Imamura et al further discloses a comparing unit that compares the first key data with the second key data, wherein the controller allows the reading or the writing of the first data based on the result of comparison performed by the comparing unit (when first identifier and the second identifier match, the controller permits access to the memory medium for the reading and writing of data) (page 1, paragraph 13). Therefore, it would have been obvious for one having ordinary skill in the art at the time the invention was made to add a step of comparing the keys to Chiba et al's disclosure. One would have been motivated to compare the keys in order to prevent an unauthorized person to access the content of the device.

Claim 3: Chiba et al and Imamura et al disclose a system for controlling key storage unit with control access to main storage as in claim 2 above, Imamura et al further discloses that if the first key data match second key data, the comparing unit authorizes the reading or the writing of the first data, and if the

first key data do not match the second key data, the comparing unit inhibits the reading and the writing of the first data (when the first identifier recorded in the storage unit does not match the second identifier recorded on the memory medium, the controller inhibits access to the memory medium for the reading and writing of data. But when first identifier and the second identifier match, the controller permits access to the memory medium for the reading and writing of data) (page 1, paragraph 13). Therefore, it would have been obvious for one having ordinary skill in the art at the time the invention was made to add a step of comparing the keys to Chiba et al's disclosure. One would have been motivated to compare the keys in order to prevent an unauthorized person to access the content of the device.

Claim 8: Chiba et al and Imamura et al disclose a system for controlling key storage unit with control access to main storage as in claim 1 above, Imamura et al further discloses a communication unit that receives the first data, the first key data, and the second key data from outside, and output the first data to the outside (when first identifier and the second identifier match, the controller permits access to the memory medium for the reading and writing of data) (page 1, paragraph 13). Therefore, it would have been obvious for one having ordinary skill in the art at the time the invention was made to add a step of displaying the output to Chiba et al's disclosure. One would have been motivated to do so in order to access the content of the device.

Claim 10: Chiba et al and Imamura et al disclose a system for controlling key storage unit with control access to main storage as in claim 1, Chiba et al further discloses that the first data area is divided into a plurality of sub data areas each containing the first data, the first key data area is divided into a plurality of sub key data areas each containing the first key data, the second key data area is divided into a plurality of sub key registers each containing the second key data (the data processing apparatus includes a main storage unit and a key storage unit for storing a main storage protection key, a reference bit, and a change bit corresponding to each block of the main storage unit.) (Column 2, lines 6-10), and Imamura et al further discloses that if the first key data stored in a desired one of the sub first key data areas matches with the second key data stored in a corresponding one of the sub second key data areas, the controller allows the reading or the writing of the first data in a corresponding of the sub data area (when first identifier and the second identifier match, the controller permits access to the memory medium for the reading and writing of data) (page 1, paragraph 13). Therefore, it would have been obvious for one having ordinary skill in the art at the time the invention was made to add a step of comparing the keys to Chiba et al's disclosure. One would have been motivated to compare the keys in order to prevent an unauthorized person to access the content of the device.

Art Unit: 2109

7. Claims 4-6 are rejected under 35 U.S.C. 103(a) as being unpatentable over **Chiba et al** (US 4589064) in view of **Imamura et al** (US 2002/0116551) as applied to claim 1 above, and in further view of **Angelo** (US 5949882).

Claim 4: **Chiba et al** and **Imamura et al** disclose a system for controlling key storage unit with control access to main storage as in claim 1, but do not explicitly disclose a second data area that stores second data that can be read and written, and that are obtained by encrypting the first key data. However **Angelo** discloses a device for allowing access to secured computer resources by utilizing a password and external encryption algorithm which further discloses a data area that stores second data that can be read and written, and that are obtained by encrypting the first key data (the computer user required to enter a plain text user password. Once entered, the user password is encrypted using the encryption algorithm contained in the external token, thereby creating a peripheral password) (column 3, lines 40-45). Therefore, it would have been obvious for one having ordinary skill in the art at the time the invention was made to add a step of encrypting the key to **Chiba et al**'s disclosure. One would have been motivated to encrypt the key in order to prevent an unauthorized person to access the content of the device and to keep data confidentiality and security in case of stolen device.

Claim 5: **Chiba et al**, **Imamura et al** and **Angelo** disclose a system for controlling key storage unit with control access to main storage as in claim 4 above, **Imamura et al** further discloses that if the first key data match second key

data, the comparing unit authorizes the reading or the writing of the second data, and if the first key data do not match the second key data, the comparing unit inhibits the reading and the writing of the first data (when the first identifier recorded in the storage unit does not match the second identifier recorded on the memory medium, the controller inhibits access to the memory medium for the reading and writing of data. But when first identifier and the second identifier match, the controller permits access to the memory medium for the reading and writing of data) (page1, paragraph 13). Therefore, it would have been obvious for one having ordinary skill in the art at the time the invention was made to add a step of comparing the keys to Chiba et al's disclosure. One would have been motivated to compare the keys in order to prevent an unauthorized person to access the content of the device.

Claim 6: Chiba et al, Imamura et al and Angelo disclose a system for controlling key storage unit with control access to main storage as in claim 5 above, Imamura et al further discloses that if the first key data match the second key data, the comparing unit authorizes the reading or the writing of the second data, and if the first key data do not match the second key data, the comparing unit authorizes only the reading but inhibits the writing of the second data (when the two device identifiers match, the process advances to step 208, whereat a check is performed to determine whether reading in accordance with the read address information is permitted. When read address information has been set, the process advances to step 209, whereat the reading of data is enable but the

writing of data is inhibited) (page 4, paragraph 87). Therefore, it would have been obvious for one having ordinary skill in the art at the time the invention was made to add a step of comparing the keys to Chiba et al's disclosure. One would have been motivated to compare the keys in order to prevent an unauthorized person to access the content of the device.

8. Claim 7 is rejected under 35 U.S.C. 103(a) as being unpatentable over Chiba et al (US 4589064) in view of Imamura et al (US 2002/0116551) as applied to claim 1 above, and in further view of Usami et al (US 6076149).

Claim 7: Chiba et al and Imamura et al disclose a system for controlling key storage unit with control access to main storage as in claim 1 above, but do not explicitly disclose a third data area that stores third data that are set when the first key data are stored, and are cleared when the first key data is reset.

However, Usami et al discloses a programmable logic device using a two bit security scheme to prevent unauthorized access, which further discloses a data area that stores third data that are set when the first key data are stored, and are cleared when the first key data is reset (to protect data against external overwriting and keeping them confidential or secure. To do so, known conventional method is to set security bit in register, and disable the operation of the input/output port when this bit is set, and enter a password when the security is to be reset or cleared) (column 1, lines 30-37). Therefore, it would have been obvious for one having ordinary skill in the art at the time the invention was made

to add a step of setting and reset a third data storage area to Chiba et al's disclosure. One would have been motivated to encrypt the key in order to prevent an unauthorized person to access the content of the device and to keep data confidentiality and security in case of stolen device.

9. Claim 9 is rejected under 35 U.S.C. 103(a) as being unpatentable over Chiba et al (US 4589064) in view of Imamura et al (US 2002/0116551) as applied to claim 1 above, and in further view of Matsuo et al (US 5974513).

Claim 9: Chiba et al and Imamura et al disclose a system for controlling key storage unit with control access to main storage as in claim 1, but do not explicitly disclose that the memory device is driven by an external electric power supply. However, Matsuo et al discloses an IC memory card having read/write inhibit capabilities, which furthers discloses that the memory device is driven by an external electric power supply (the memory control portion is always in the inhibit mode when electric power is supplied from outside) (column 2, lines 1-3). Therefore, it would have been obvious for one having ordinary skill in the art at the time the invention was made to drive the device by an external electric power supply to Chiba et al's disclosure. One would have been motivated to do so in order to get a low power usage.

Art Unit: 2109

10. Claim 14 is rejected under 35 U.S.C. 103(a) as being unpatentable over Chiba et al (US 4589064) in view of Imamura et al (US 2002/0116551) as applied to claim 1 above, and in further view of Yasu et al (US 5912849).

Claim 14: Chiba et al and Imamura et al disclose a system for controlling key storage unit with control access to main storage as in claim 1, but do not explicitly disclose the first data area and the first key data area are composed of a ferroelectric memory that holds the data by means of remnant polarization. However, Yasu et al discloses a write protection device for a non-volatile memory, which further discloses that the data storage area is composed of a ferroelectric memory (the ferroelectric memory is usable as a RAM even though it is a non-volatile memory) (column 2, lines 53-55). Therefore, it would have been obvious for one having ordinary skill in the art at the time the invention was made to store the data in a ferroelectric memory in Chiba et al's disclosure. One would have been motivated to do so in order to get at least one of the many advantages of the ferroelectric memory such as: lower power usage, faster write speed and a much greater maximum number (exceeding 10^{16} for 3.3 V devices) of write-erase cycles.

11. Claims 15, 23 are rejected under 35 U.S.C. 103(a) as being unpatentable over anticipated by Chiba et al (US 4589064) in view of Matsuo et al (US 5974513).

Claim 15: Chiba et al discloses a system for controlling key storage unit with control access to main storage comprising:

a. A memory device that includes a nonvolatile first data area that stores first data that are not encrypted and that can be read and written (the data processing apparatus includes a main storage unit) (column 2, lines 6-7);

b. A nonvolatile first key data area that stores first key data that can be written but can not be read (the data processing apparatus includes a main storage unit and a key storage unit for storing a main storage protection key) (column 2, lines 6-8);

c. A nonvolatile second key data area that stores second key data that can be written but can not be read (the data processing apparatus includes a main storage unit and a key storage unit for storing a main storage protection key) (column 2, lines 6-8);

But does not explicitly disclose a controller that allows reading or writing of the first data when the first key data matches with the second key data. However **Matsuo et al** disclose an IC memory card having read/write inhibit capabilities, which further discloses:

a. And a controller that allows reading or writing of the first data when the first key data matches with the second key data (a memory control portion for controlling writing into the semiconductor memory in accordance with the instruction) (column 1, lines 60-63);

b. A writing unit that writes the first data into the first data area and the first key data into the first key data area (a memory control portion for controlling

writing into the semiconductor memory in accordance with the instruction from the read-write device) (column 1, lines 60-63);

c. A first interface unit that is used for transmission and reception of data between the writing unit and the memory device (a connector portion for uniting with read-write device) (column 1, lines 57-60);

d. A reading/writing unit that writes the second key data into the second key data area, and accesses the first data area for reading and writing the first data (a memory control portion for controlling writing into the semiconductor memory in accordance with the instruction from the read-write device) (column 1, lines 60-63);

e. And a second interface unit that is used for transmission and reception of data between the reading/writing unit and the memory device (a connector portion for uniting with read-write device) (column 1, lines 57-60);

Therefore, it would have been obvious for one having ordinary skill in the art at the time the invention was made to add a controller to Chiba et al's disclosure.

One would have been motivated to control the device in order to prevent an unauthorized person to access the content of the device.

Claim 23: Chiba et al and Matsuo et al disclose a system for controlling key storage unit with control access to main storage as in claim 15 above, Matsuo et al further discloses that the memory device is driven by an external electric power supply (the memory control portion is always in the inhibit mode when

electric power is supplied from outside) (column 2, lines 1-3). Therefore, it would have been obvious for one having ordinary skill in the art at the time the invention was made to drive the device by an external electric power supply to Chiba et al's disclosure. One would have been motivated to do so in order to get a low power usage.

12. Claims 16-17, 22, 24 are rejected under 35 U.S.C. 103(a) as being unpatentable over anticipated by Chiba et al (US 4589064) in view of Matsuo et al (US 5974513) as applied to claim 15 above, and in further view of Imamura et al (US 2002/0116551).

Claim 16: Chiba et al and Matsuo et al disclose a system for controlling key storage unit with control access to main storage as in claim 15 above, but do not explicitly disclose a comparing unit that compares the first key data with the second key data, wherein the controller allows the reading or the writing of the first data based on the result of comparison performed by the comparing unit. However, Imamura et al disclose an IC memory card having read/write inhibit capabilities, which further discloses a comparing unit that compares the first key data with the second key data, wherein the controller allows the reading or the writing of the first data based on the result of comparison performed by the comparing unit (when first identifier and the second identifier match, the controller permits access to the memory medium for the reading and writing of data) (page 1, paragraph 13). Therefore, it would have been obvious for one having ordinary skill in the art at the time the invention was made to add a step of

comparing the keys to Chiba et al's disclosure. One would have been motivated to compare the keys in order to prevent an unauthorized person to access the content of the device.

Claim 17: Chiba et al, Matsuo et al, and Imamura et al disclose a system for controlling key storage unit with control access to main storage as in claim 16 above, Imamura et al further disclose an IC memory card having read/write inhibit capabilities, which further discloses that if the first key data match second key data, the comparing unit authorizes the reading or the writing of the first data, and if the first key data do not match the second key data, the comparing unit inhibits the reading and the writing of the first data (when the first identifier recorded in the storage unit does not match the second identifier recorded on the memory medium, the controller inhibits access to the memory medium for the reading and writing of data. But when first identifier and the second identifier match, the controller permits access to the memory medium for the reading and writing of data) (page 1, paragraph 13). Therefore, it would have been obvious for one having ordinary skill in the art at the time the invention was made to add a step of comparing the keys to Chiba et al's disclosure. One would have been motivated to compare the keys in order to prevent an unauthorized person to access the content of the device.

Claim 22: Chiba et al and Matsuo et al disclose a system for controlling key storage unit with control access to main storage as in claim 15 above, but do not explicitly disclose that the memory includes a communication unit that receives

the first data, the first key data, and the second key data from the writing unit via the first interface unit, outputs the first data to the reading/writing unit via the second interface. However, Imamura et al disclose an IC memory card having read/write inhibit capabilities, which further discloses a communication unit that receives the first data, the first key data, and the second key data from writing unit, and output the first data to the reading/writing unit (when first identifier and the second identifier match, the controller permits access to the memory medium for the reading and writing of data) (page 1, paragraph 13). Therefore, it would have been obvious for one having ordinary skill in the art at the time the invention was made to add a step of displaying the output to Chiba et al's disclosure. One would have been motivated to do so in order to access the content of the device.

Claim 24: Chiba et al and Matsuo et al disclose a system for controlling key storage unit with control access to main storage as in claim 15, Chiba et al further discloses that the first data area is divided into a plurality of sub data areas each containing the first data, the first key data area is divided into a plurality of sub key data areas each containing the first key data, the second key data area is divided into a plurality of sub key registers each containing the second key data (the data processing apparatus includes a main storage unit and a key storage unit for storing a main storage protection key, a reference bit, and a change bit corresponding to each block of the main storage unit.) (Column 2, lines 6-10), but do not explicitly disclose that if the first key data stored in a desired one of the sub first key data areas matches with the second key data

stored in a corresponding one of the sub second key data areas, the controller allows the reading or the writing of the first data in a corresponding of the sub data area. However, Imamura et al disclose an IC memory card having read/write inhibit capabilities, which further discloses that if the first key data stored in a desired one of the sub first key data areas matches with the second key data stored in a corresponding one of the sub second key data areas, the controller allows the reading or the writing of the first data in a corresponding of the sub data area (when first identifier and the second identifier match, the controller permits access to the memory medium for the reading and writing of data) (page 1, paragraph 13). Therefore, it would have been obvious for one having ordinary skill in the art at the time the invention was made to add a step of comparing the keys to Chiba et al's disclosure. One would have been motivated to compare the keys in order to prevent an unauthorized person to access the content of the device.

13. Claim 18 is rejected under 35 U.S.C. 103(a) as being unpatentable over Chiba et al (US 4589064) in view of Matsuo et al (US 5974513) as applied to claim 15 above, and in further view of Angelo (US 5949882).

Claim 18: Chiba et al and Matsuo et al disclose a system for controlling key storage unit with control access to main storage as in claim 15, but do not explicitly disclose a second data area that stores second data that can be read and written, and that are obtained by encrypting the first key data. However

Angelo discloses a method and apparatus for allowing access to secured computer resources by utilizing a password and external encryption algorithm which furthers discloses a data area that stores second data that can be read and written, and that are obtained by encrypting the first key data (the computer user required to enter a plain text user password. Once entered, the user password is encrypted using the encryption algorithm contained in the external token, thereby creating a peripheral password) (column 3, lines 40-45).

Therefore, it would have been obvious for one having ordinary skill in the art at the time the invention was made to add a step of encrypting the key to Chiba et al's disclosure. One would have been motivated to encrypt the key in order to prevent an unauthorized person to access the content of the device and to keep the data confidential and secure in case of stolen device.

14. Claims 19-20 are rejected under 35 U.S.C. 103(a) as being unpatentable over Chiba et al (US 4589064) in view of Matsuo et al (US 5974513) as applied to claim 15 above, and in further view of Angelo (US 5949882), and Imamura et al (US 2002/0116551).

Claim 19: Chiba et al, Matsuo et al and Angelo disclose a system for controlling key storage unit with control access to main storage as in claim 18 above, but do not explicitly disclose that if the first key data match second key data, the comparing unit authorizes the reading or the writing of the second data, and if the first key data do not match the second key data, the comparing unit inhibits the

reading and the writing of the first data. However, Imamura et al disclose an IC memory card having read/write inhibit capabilities, which further discloses that if the first key data match second key data, the comparing unit authorizes the reading or the writing of the second data, and if the first key data do not match the second key data, the comparing unit inhibits the reading and the writing of the first data (when the first identifier recorded in the storage unit does not match the second identifier recorded on the memory medium, the controller inhibits access to the memory medium for the reading and writing of data. But when first identifier and the second identifier match, the controller permits access to the memory medium for the reading and writing of data) (page 1, paragraph 13).

Therefore, it would have been obvious for one having ordinary skill in the art at the time the invention was made to add a step of comparing the keys to Chiba et al's disclosure. One would have been motivated to compare the keys in order to prevent an unauthorized person to access the content of the device.

Claim 20: Chiba et al, Matsuo et al, Angelo and Imamura et al disclose a system for controlling key storage unit with control access to main storage as in claim 19 above, Imamura et al further discloses that if the first key data match the second key data, the comparing unit authorizes the reading or the writing of the second data, and if the first key data do not match the second key data, the comparing unit authorizes only the reading but inhibits the writing of the second data (when the two device identifiers match, the process advances to step 208, whereat a check is performed to determine whether reading in accordance with

the read address information is permitted. When read address information has been set, the process advances to step 209, whereat the reading of data is enable but the writing of data is inhibited) (page 4, paragraph 87). Therefore, it would have been obvious for one having ordinary skill in the art at the time the invention was made to add a step of comparing the keys to Chiba et al's disclosure. One would have been motivated to compare the keys in order to prevent an unauthorized person to access the content of the device.

15. Claim 21 is rejected under 35 U.S.C. 103(a) as being unpatentable over Chiba et al (US 4589064) in view of Matsuo et al (US 5974513) as applied to claim 15 above, and in further view of Usami et al (US 6076149).

Claim 21: Chiba et al and Matsuo et al disclose a system for controlling key storage unit with control access to main storage as in claim 15, but do not explicitly disclose a third data area that stores third data that are set when the first key data are stored, and are cleared when the first key data is reset.

However, Usami et al discloses a programmable logic device using a two bit security scheme to prevent unauthorized access, which furthers discloses a data area that stores third data that are set when the first key data are stored, and are cleared when the first key data is reset (to protect data against external overwriting and keeping them confidential or secure. To do so, known conventional method is to set security bit in register, and disable the operation of the input/output port when this bit is set, and enter a password when the security

is to be reset or cleared) (column 1, lines 30-37). Therefore, it would have been obvious for one having ordinary skill in the art at the time the invention was made to add a step of setting and reset a third data storage area to Chiba et al's disclosure. One would have been motivated to encrypt the key in order to prevent an unauthorized person to access the content of the device and to keep data confidentiality and security in case of stolen device.

16. Claim 28 is rejected under 35 U.S.C. 103(a) as being unpatentable over Chiba et al (US 4589064) in view of Matsuo et al (US 5974513) as applied to claim 15 above, and in further view of Yasu et al (US 5912849).

Claim 28: Chiba et al and Matsuo et al disclose a system for controlling key storage unit with control access to main storage as in claim 15, but do not explicitly disclose the first data area and the first key data area are composed of a ferroelectric memory that holds the data by means of remnant polarization. However, Yasu et al discloses a write protection device for a non-volatile memory, which furthers discloses that the data storage area is composed of a ferroelectric memory (the ferroelectric memory is usable as a RAM even though it is a non-volatile memory) (column 2, lines 53-55). Therefore, it would have been obvious for one having ordinary skill in the art at the time the invention was made to store the data in a ferroelectric memory in Chiba et al's disclosure. One would have been motivated to do so in order to get at least one of the many advantages of the ferroelectric memory such as: lower power usage, faster write

speed and a much greater maximum number (exceeding 10^{16} for 3.3 V devices) of write-erase cycles.

17. Claim 11 is rejected under 35 U.S.C. 103(a) as being unpatentable over anticipated by Chiba et al (US 4589064) in view of Imamura et al (US 2002/0116551) as applied to claim 10 above, and in further view of Yoshimaru (US 4641294).

Claim 11: Chiba et al and Imamura et al disclose a system for controlling key storage unit with control access to main storage as in claim 10 above, but do not explicitly disclose that all the sub data areas have same memory capacity. However, Yoshimaru discloses a method and apparatus for performing a memory operation on a fixed length block of data on a memory disk, which further discloses that all the sub data areas have same memory capacity (there is provided a memory disk apparatus wherein a plurality of track block having the same track length is assigned to disk track) (column 1, lines 50-63). Therefore, it would have been obvious for one having ordinary skill in the art at the time the invention was made to have a fixed memory capacity in Chiba et al's disclosure. One would have been motivated to do so in order to improve the recording density of data on the memory disk.

18. Claims 12-13 are rejected under 35 U.S.C. 103(a) as being unpatentable over anticipated by Chiba et al (US 4589064) in view of Imamura et al (US 2002/0116551) as applied to claim 10 above, and in further view of Schwartz et al (US 4654781).

Claim 12: Chiba et al and Imamura et al disclose a system for controlling key storage unit with control access to main storage as in claim 10 above, but do not explicitly disclose that each of the sub data area has a different memory capacity. However, Schwartz et al discloses a byte addressable memory for variable length instruction and data, which further discloses that each of the sub data area has a different memory capacity (twelve bytes of digital information are listed illustrating a typical mixture of variable length instructions with variable numbers of operand specifiers and variable size data types which may be 8, 16, 32 or 64 bits long that may be stored in a memory array) (column 4, lines 25-30).

Therefore, it would have been obvious for one having ordinary skill in the art at the time the invention was made to have a variable memory capacity in Chiba et al's disclosure. One would have been motivated to do so in order to achieve maximum utilization of the memory storage space available.

Claim 13: Chiba et al and Imamura et al disclose a system for controlling key storage unit with control access to main storage as in claim 10 above, but do not explicitly disclose that memory capacity of each of the sub data area is set based on a length of data to be stored in the sub data area. However, Schwartz et al discloses a byte addressable memory for variable length instruction and data, which further discloses that the memory capacity of each of the sub data area is set based on a length of data to be stored in the sub data area (twelve bytes of digital information are listed illustrating a typical mixture of variable length instructions with variable numbers of operand specifiers and variable size data

types which may be 8, 16, 32 or 64 bits long that may be stored in a memory array) (column 4, lines 25-30). Therefore, it would have been obvious for one having ordinary skill in the art at the time the invention was made to have a variable memory capacity in Chiba et al's disclosure. One would have been motivated to do so in order to achieve maximum utilization of the memory storage space available.

19. Claim 25 is rejected under 35 U.S.C. 103(a) as being unpatentable over anticipated by Chiba et al (US 4589064) in view of Matsuo et al (US 5974513), Imamura et al (US 2002/0116551) as applied to claim 15 above, and in further view of Yoshimaru (US 4641294).

Claim 25: Chiba et al, Matsuo et al and Imamura et al disclose a system for controlling key storage unit with control access to main storage as in claim 24 above, but do not explicitly disclose that all the sub data areas have same memory capacity. However, Yoshimaru discloses a method and apparatus for performing a memory operation on a fixed length block of data on a memory disk, which further discloses that all the sub data areas have same memory capacity (there is provided a memory disk apparatus wherein a plurality of track block having the same track length is assigned to disk track) (column 1, lines 50-63). Therefore, it would have been obvious for one having ordinary skill in the art at the time the invention was made to have a fixed memory capacity in Chiba et

Art Unit: 2109

al's disclosure. One would have been motivated to do so in order to improve the recording density of data on the memory disk.

20. Claims 26-27 are rejected under 35 U.S.C. 103(a) as being unpatentable over anticipated by Chiba et al (US 4589064) in view of Matsuo et al (US 5974513), Imamura et al (US 2002/0116551) as applied to claim 15 above, and in further view of Schwartz et al (US 4654781).

Claim 26: Chiba et al, Matsuo et al and Imamura et al disclose a system for controlling key storage unit with control access to main storage as in claim 24 above, but do not explicitly disclose that each of the sub data area has a different memory capacity. However, Schwartz et al discloses a byte addressable memory for variable length instruction and data, which further discloses that each of the sub data area has a different memory capacity (twelve bytes of digital information are listed illustrating a typical mixture of variable length instructions with variable numbers of operand specifiers and variable size data types which may be 8, 16, 32 or 64 bits long that may be stored in a memory array) (column 4, lines 25-30). Therefore, it would have been obvious for one having ordinary skill in the art at the time the invention was made to have a variable memory capacity in Chiba et al's disclosure. One would have been motivated to do so in order to achieve maximum utilization of the memory storage space available.

Claim 27: Chiba et al, Matsuo et al and Imamura et al disclose a system for controlling key storage unit with control access to main storage as in claim 24

above, but do not explicitly disclose that memory capacity of each of the sub data area is set based on a length of data to be stored in the sub data area.

However, Schwartz et al discloses a byte addressable memory for variable length instruction and data, which further discloses that the memory capacity of each of the sub data area is set based on a length of data to be stored in the sub data area (twelve bytes of digital information are listed illustrating a typical mixture of variable length instructions with variable numbers of operand specifiers and variable size data types which may be 8, 16, 32 or 64 bits long that may be stored in a memory array) (column 4, lines 25-30). Therefore, it would have been obvious for one having ordinary skill in the art at the time the invention was made to have a variable memory capacity in Chiba et al's disclosure. One would have been motivated to do so in order to achieve maximum utilization of the memory storage space available.

Conclusion

21. The prior art made of record and not relied upon is considered pertinent to applicant's disclosure.

- d. Fukuzumi, (US 6079019) IC memory Card.
- e. Kimura, (US 5237609) Portable secure semiconductor memory device.
- f. Watanaba et al, (US 4849614) Composite IC card.
- g. Lijima, (US 4985615) Portable electronic apparatus having data for limiting memory access.

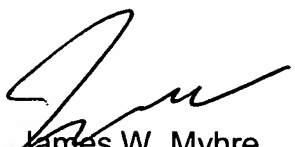
Art Unit: 2109

Any inquiry concerning this communication or earlier communications from the examiner should be directed to Fatoumata Traore whose telephone number is (571) 270-1685. The examiner can normally be reached Monday through Thursday from 7:30 a.m. to 4:30 p.m. and every other Friday from 7:30 a.m. to 3:30 p.m.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Jim W. Myhre, can be reached on (571) 272 6722. The fax phone number for Formal or Official faxes to Technology Center 2100 is (571) 273-8300. Draft or Informal faxes, which will not be entered in the application, may be submitted directly to the examiner at (571) 274-1685.

Any inquiry of a general nature or relating to the status of this application or proceeding should be directed to the Group Receptionist whose telephone number is (571) 272-2100.

FT
April 18, 2007


James W. Myhre
Supervisory Patent Examiner